REMARKS

This is in full and timely response to the non-final Office Action mailed on November 18, 2002. Reexamination in light of the following remarks is respectfully requested.

Claims 1-18 and 22-46 are pending in this application, with claims 1, 22, 24, 26 and 44 being independent. No new matter has been added.

Interview

Applicant gratefully wishes to thank the Examiner for extending the courtesy of granting and conducting on December 19, 2002, a personal interview to discuss the rejection made within the non-final Office Action of November 18, 2002.

Rejection Under 35 U.S.C. 103

Claims 24 and 25 were rejected under 35 U.S.C. 103 as being allegedly being obvious over U.S. Patent 6,385,591 issued to Mankoff in view of Sutherland ("*Promotion Profile*", Marketing & Media Decisions, Vol. 24, No. 10, October 1989, p. 103) and U.S. Patent 6,298,446 issued to Schreiber et al. (Schreiber).

Claims 1-6, 9-18, 22 and 23 were rejected under 35 U.S.C. 103 as being allegedly being obvious over Mankoff in view of

Sutherland and Schreiber, and in further view of "Emaginet Plans To 'Push' Its Way Into Consumer Mindset, Pocketbook," Interactive Marketing News, v4, n22, May 30, 1997 (Emaginet).

Claims 7 and 8 were rejected under 35 U.S.C. 103 as being allegedly being obvious over Mankoff in view of Sutherland and Schreiber, in view of Emaginet, and in further view of U.S. Patent No. 6,006,269 issued to Phaal.

These rejections are respectfully traversed for at least the following reasons.

Independent claim 24 is drawn to a method of secure electronic coupon distribution, claim 25 is dependent upon claim 24. Claim 24 includes the steps of associating a Uniform Resource Locator (URL) including a promotional code with a coupon; displaying the coupon to a user; disabling access to the URL by the user; and invoking the URL with a browser to thereby enable the user to redeem the coupon. Specifically, page 17, lines 21-28 of the specification provides that:

> Client application 28 disables access to the invoked URL/code. For example, moving the mouse arrow over the coupon/ad does not cause the URL to be displayed, nor is "right-button clicking" operative to allow capture of the URL. Accordingly, *the specified URL (and code) is*

neither displayed nor available, and cannot be discovered by, for example, "right-clicking" on coupon display 76, like conventional web-based e-coupon distribution systems.

Mankoff arguably provides that an electronic or "virtual" coupon is obtained when a user selects a given link in a Web page being displayed on a client machine (column 1, lines 44-47). Arguably, column 1, lines 50-58 of Mankoff teaches contact information associated with the coupon provider (e.g., address, web site URL, map and e-mail information) as automatically written to the PDA contact file.

Mankoff, at column 2, lines 61-65, arguably teaches that the web server supports files (collectively referred to as a web site) in the form of hypertext documents and objects, and that a network path to a server is identified by a so-called Uniform Resource Locator (URL).

In spite of the teachings within Mankoff, that reference fails to disclose, teach or suggest the claimed feature of disabling access ***to the URL*** by the user. The non-final Office Action recognizes that this feature is absent within Mankoff.

Sutherland arguably makes a reference to "electronic coupon scanning." Nevertheless, Sutherland is silent as to the claimed feature of disabling access to the URL by the user.

Emaginet is also is silent as to the claimed feature of disabling access to the URL by the user.

Phaal arguably teaches an admission control system that includes a buffer for storing a URL (column 7, lines 15-16). Nevertheless, Phaal fails to disclose, teach or suggest the claimed feature of disabling access to the URL by the user.

Schreiber arguably teaches a method and system for copyright protection of digital images. Schreiber arguably teaches that SafeMedia includes enhanced system control for preventing screen capture by disabling a clipboard (column 2, lines 27-30).

Schreiber arguably teaches that that other prior art techniques for protecting digital images use Java applets within web browsers to disable the menu that pops up when a user right clicks on a displayed image within his web browser (column 2, lines 37-40).

Schreiber arguably teaches that the disablement of the user's ability to save an image being displayed and the non-

enablement of the user to save image data (column 7, lines 58-60).

Schreiber arguably teaches that some URL's do not correspond to existing web page files, but instead contain instructions, such as CGI script instructions or Visual Basic instructions, for generating dynamic web pages, such as active server pages. When a user opens such an URL, the server computer typically generates a web page dynamically, and sends the generated web page to the client computer. Column 14, lines 55-61.

Schreiber arguably teaches that in response to a user selecting a URL with a CGI script or such other script, client computer 106 issues an HTTP request to server computer 100 that includes instructions for generating a web page (column 16, lines 6-9).

Schreiber arguably teaches that at step 606 the user opens a URL for an active server page in his web browser, or another such URL that includes a request for dynamically generating a web page (column 16, line 67 to column 17, line 3).

Schreiber arguably teaches that at step 1002 a user opens a URL for a web page in his web browser (column 21, lines 6-7).

Column 25, lines 34-37 of Schreiber further provides for parameters that are disabled so that they cannot be edited. They indicate the DLL version of the copyright protection software, the Netscape version and the ActiveX version, respectively.

Also described within Schreiber are the disablement of the DELETE button (column 26, lines 46-47) and the disablement of the REMOVE button (column 27, lines 18-25).

In spite of the above-noted teachings, the claimed feature of disabling access to the URL by the user is not found within Schreiber. Instead, preferred embodiment of the Schreiber is drawn to a method for protecting digital images distributed over a network (column 3, lines 37-39), and is not drawn to the disablement of access to the URL.

The non-final Office Action also fails to highlight the particular teaching within the cited prior art that is relied upon for the claimed feature of disabling access to the URL by the user.

Withdrawal of these rejections and allowance of the claims is respectfully requested.

Newly added claims

Previously presented claims 1-23 are provided as newly added claims 26-48.

Like claim 1, claim 26 and the claims dependent thereon include the step of collecting device information from a device of a client system without obtaining information sufficient to specifically identify the user.

Like claim 19, claim 44 and the claims dependent thereon include means for collecting user information from a user of a remote client system indicative of one or more demographic characteristics of the user without obtaining information sufficient to specifically identify the user.

This feature is supported within the specification as originally filed. For example, figure 4 of the specification as originally filed depicts step 107. Within that step, personal information such as the user's name, e-mail address, residence address, social security number, telephone number, and the like is not obtained (page 19, lines 34-36). The user ID does not specifically identify the user personally, but rather, more accurately associates a physical machine defining

client system 14 with user profile information obtained during registration (page 10, lines 9-12). Significantly, however, the user is not personally identified nor is it even possible (e.g., through the "hacking" of server system 12) to identify the user personally, as such information is not even collected from the user (page 10, lines 19-22). This feature is not found within the cited prior art.

In particular, Emaginet arguably provides a general discussion regarding electronic coupons. However, Emaginet fails to disclose, teach or suggest the step of collecting device information from a device of a client system without obtaining information sufficient to specifically identify the user. Instead, Emaginet merely proposes, without providing specific details, that customers who register their preferences an buying habits at Emaginet's website can download an assortment of offers.

The claimed feature of collecting device information from a device of a client system without obtaining information sufficient to specifically identify the user is also not found within Mankoff, Sutherland, Schreiber and Phaal, either individually or as a whole.

Allowance of the claims is respectfully requested.

Conclusion

For the foregoing reasons, all the claims now pending in the present application are allowable, and the present application is in condition for allowance. Accordingly, favorable reexamination and reconsideration of the application in light of the amendments and remarks is courteously solicited.

If the Examiner has any comments or suggestions that could place this application in even better form, the Examiner is requested to telephone the undersigned attorney at the below-listed number.

Respectfully submitted,

DATE: December 20, 2002

Ronald P. Kananen
Reg. No. 24,104

RADER, FISHMAN & GRAUER PLLC
Lion Building
1233 20th Street, N.W.
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751

APPENDIX

IN THE CLAIMS

1. The method of claim 24 further including the steps of:

collecting device information from a device of a client system without obtaining information sufficient to specifically identify the user;

associating a device ID with the device information at a main server system;

selecting said coupon according to the device ID to thereby identify the coupon appropriate for said user based on the device information; and,

transmitting the selected coupon from the main server system to the client system.

2. The method of claim 1 wherein said collecting step comprises the optional substep of:

obtaining from the remote user demographic characteristics including at least one of a postal zip code associated with the user and a state in which the user resides.

3. The method of claim 1 further including the step of:

associating the device ID with a remote client system.

4. The method of claim 3 further including the step of:

generating a printed version of one of the transmitted coupon at the remote client system.

5. The method of claim 3 further including the step of:

transmitting a request from the client system to the server system to perform said selecting step wherein the request includes the device ID.

6. The method of claim 5 wherein said request transmitting step includes the substep of:

automatically including the device ID in the request without any intervention by a remote user of the client system.

7. The method of claim 5 wherein said request transmitting step occurs automatically without any intervention by a remote user.

8. The method of claim 7 wherein said request transmitting step occurs at predetermined intervals.

9. The method of claim 3 wherein the remote client system operates in accordance with an operating system characterized by a graphical user interface (GUI), said method further including the steps of:

displaying an icon visible to the user in a first display state; and,

displaying the icon in a second display state different from the first display state when a new coupon is available for the user.

10. The method of claim 9 wherein the second display state is a flashing display state.

11. The method of claim 3 wherein said transmitting step includes the substeps of:

encrypting coupon data corresponding to the selected coupon at the server system in accordance with a server system encryption strategy; and,

sending the server-encrypted coupon data to the client system.

12. The method of claim 11 further including the step of:

receiving the server-encrypted coupon data at the client system;

encrypting the server-encrypted coupon data in accordance with a client system encryption strategy to thereby generate doubly-encrypted coupon data; and,

storing the doubly-encrypted coupon data on the client system.

13. The method of claim 12 further including the steps of:

decrypting the doubly-encrypted coupon data at the client system; and,

generating a printed version of one of the selected coupon at the remote client system.

14. The method of claim 3 further comprising the steps of:

transmitting advertising data to the client system; and,

displaying at least a portion of the transmitted advertising data on a display portion of the remote client system.

15. The method of claim 14 wherein the advertising data comprises a plurality of advertising impressions, and, wherein said displaying step comprises the substep of:

selecting one of the plurality of advertising impressions as a function of a selected subcategory of coupons available on the remote client system.

16. The method of claim 3 further comprising the steps of:

detecting events occurring at the remote client system;

storing the detected events in a user history file; and,

transmitting the user history file to the server system.

17. The method of claim 16 wherein said detecting step includes the substeps of:

determining when one of a plurality of advertising impressions has been displayed on a display portion of the remote client system; and,

determining a sponsor identification of the advertising impression.

18. The method of claim 16 wherein the storing step comprises the substep of:

encrypting the detected events to thereby generate encrypted user event information; and,

writing the encrypted user event information to the client system.

19. (canceled).

20. (canceled).

21. (canceled).

22. The method of claim 24 further including the steps of:

collecting device information from a device on a network;

associating a device ID with the device information;

selecting said coupon according to the device ID;

encrypting coupon data corresponding to the selected coupon; and,

transmitting the encrypted coupon data from the main server system to the client system.

23. The method of claim 22 further including the step of:

decrypting the encrypted coupon data to recover the selected coupon.

24. A method of secure electronic coupon distribution comprising the steps of:

associating a Uniform Resource Locator (URL) including a promotional code with a coupon;

displaying the coupon to a user;

disabling access to the URL by the user; and,

invoking the URL with a browser to thereby enable the user to redeem the coupon.

25. The method of claim 24 wherein said invoking step includes the substep of selecting the coupon by one of clicking on the displayed coupon and clicking on an object different than the coupon displayed to the user.

Please add the following new claims.

26. (new) The method of operating an electronic coupon distribution system comprising the steps of:

collecting device information from a device of a client system without obtaining information sufficient to specifically identify the user;

associating a device ID with the device information at a main server system;

selecting said coupon according to the device ID to thereby identify the coupon appropriate for said user based on the device information; and,

transmitting the selected coupon from the main server system to the client system.

27. (new) The method of claim 26 wherein said collecting step comprises the substep of:

obtaining from the remote user demographic characteristics including at least one of a postal zip code associated with the user and a state in which the user resides.

28. (new) The method of claim 26 further including the step of:

associating the user ID with the remote client system.

29. (new) The method of claim 28 further including the step of:

generating a printed version of one of the transmitted coupons at the remote client system that includes the user ID.

30. (new) The method of claim 28 further including the step of:

transmitting a request from the client system to the server system to perform said selecting step wherein the request includes the user ID.

31. (new) The method of claim 30 wherein said request transmitting step includes the substep of:

automatically including the user ID in the request without any intervention by the remote user of the client system.

32. (new) The method of claim 30 wherein said request transmitting step occurs automatically without any intervention by the remote user.

33. (new) The method of claim 32 wherein said request transmitting step occurs at predetermined intervals.

34. (new) The method of claim 28 wherein the remote client system operates in accordance with an operating system characterized by a graphical user interface (GUI), said method further including the steps of:

displaying an icon visible to the user in a first display state; and,

displaying the icon in a second display state different from the first display state when new coupon are available for the user.

35. (new) The method of claim 34 wherein the second display state is a flashing display state.

36. (new) The method of claim 28 wherein said transmitting step includes the substeps of:

encrypting coupon data corresponding to the selected coupons at the server system in accordance with a server system encryption strategy; and,

sending the server-encrypted coupon data to the client system.

37. (new) The method of claim 36 further including the step of:

receiving the server-encrypted coupon data at the client system;

encrypting the server-encrypted coupon data in accordance with a client system encryption strategy to thereby generate doubly-encrypted coupon data; and,

storing the doubly-encrypted coupon data on the client system.

38. (new) The method of claim 37 further including the steps of:

decrypting the doubly-encrypted coupon data at the client system; and,

generating a printed version of one of the selected coupons at the remote client system.

39. (new) The method of claim 28 further comprising the steps of:

transmitting advertising data to the client system; and,

displaying at least a portion of the transmitted advertising data on a display portion of the remote client system.

40. (new) The method of claim 39 wherein the advertising data comprises a plurality of advertising impressions, and, wherein said displaying step comprises the substep of:

selecting one of the plurality of advertising impressions as a function of a selected subcategory of coupons available on the remote client system.

41. (new) The method of claim 28 further comprising the steps of:

detecting events occurring at the remote client system;

storing the detected events in a user history file; and,

transmitting the user history file to the server system.

42. (new) The method of claim 41 wherein said detecting step includes the substeps of:

determining when one of the plurality of advertising impressions has been displayed on a display portion of the remote client system; and,

determining a sponsor identification of the advertising impression.

43. (new) The method of claim 41 wherein the storing step comprises the substep of:

encrypting the detected events to thereby generate encrypted user event information; and,

writing the encrypted user event information to the client system.

44. (new) A coupon distribution system, comprising:

means for collecting user information from a user of a remote client system indicative of one or more demographic characteristics of the user without obtaining information sufficient to specifically identify the user;

means for associating a user ID with the user information at a main server system;

means for selecting coupons according to the user ID to thereby identify coupons appropriate for the user based on the user's demographic characteristics; and,

means for transmitting the selected coupons from the server system to the client system.

45. (new) The system of claim 44 wherein said collecting means includes means for obtaining from the remote user demographic characteristics including at least one of a postal zip code associated with the user and a state in which the user resides.

46. (new) The system of claim 45 further including means for associating the user ID with the remote client system.